

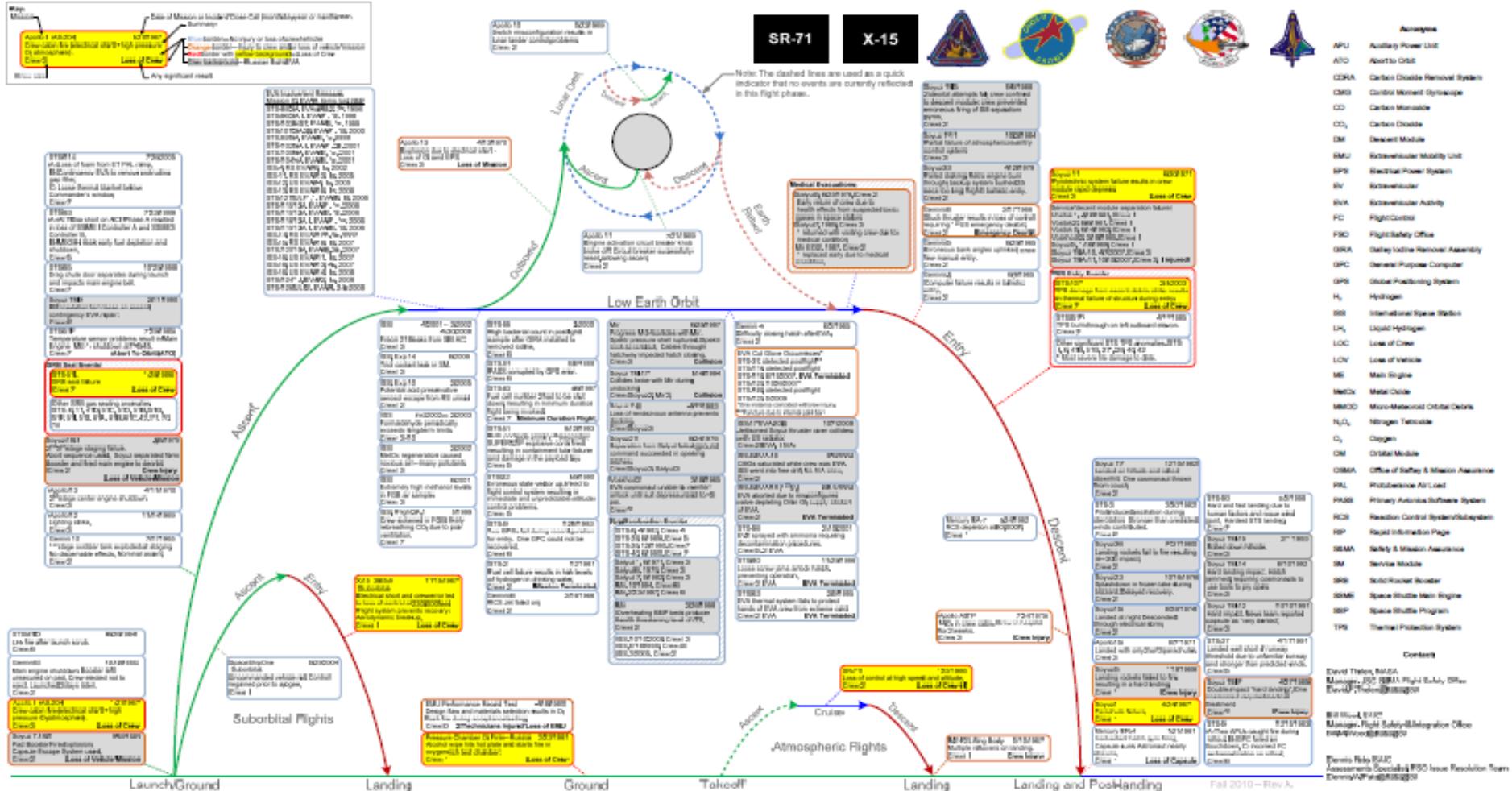


NASA Hazard Analysis Process

George Deckert
Johnson Space Center
Safety, Reliability and Mission Assurance Directorate

Significant Incidents and Close Calls in Human Spaceflight

A Product of the JSC S&MA Flight Safety Office



The Significant Incidents and Close Calls in Human Spaceflight graphic is primarily focused on human spaceflight incidents that have occurred while a crew was aboard a space vehicle. It includes suborbital, orbital, and lunar missions. The low ground faculty events and free-atmospheric flight events are included due to the significance of the events to spaceflight. The pressure chamber O₂ fire in Russia occurred prior to the loss of the Apollo 1 crew in 1967 and could have served as a lesson learned had it been known in the US. The EMU fire resulted in the redesign of the EMU and heightened awareness of design and materials selection for man-rated

systems using a pure O₂ environment. The O₂/F₂ fire likely occurred during the development of the space shuttle and yielded human engineering lessons learned. The O₂/F₂ accident is the highest rated event on record that has survivability and it represents the demonstrated limit of crew survival with currently fielded technologies. Note: This document is in work in progress. It is continually under review and frequently updated. Please direct comments and questions to the Flight Safety Office contacts at right.

Fall 2010 – Rev A

David Thelen, NASA
Manager, JSC S&MA Flight Safety Office
david.thelen@nasa.gov

Bill Ladd, NASA
Manager, Flight Safety & Reliability Office
bill.ladd@nasa.gov

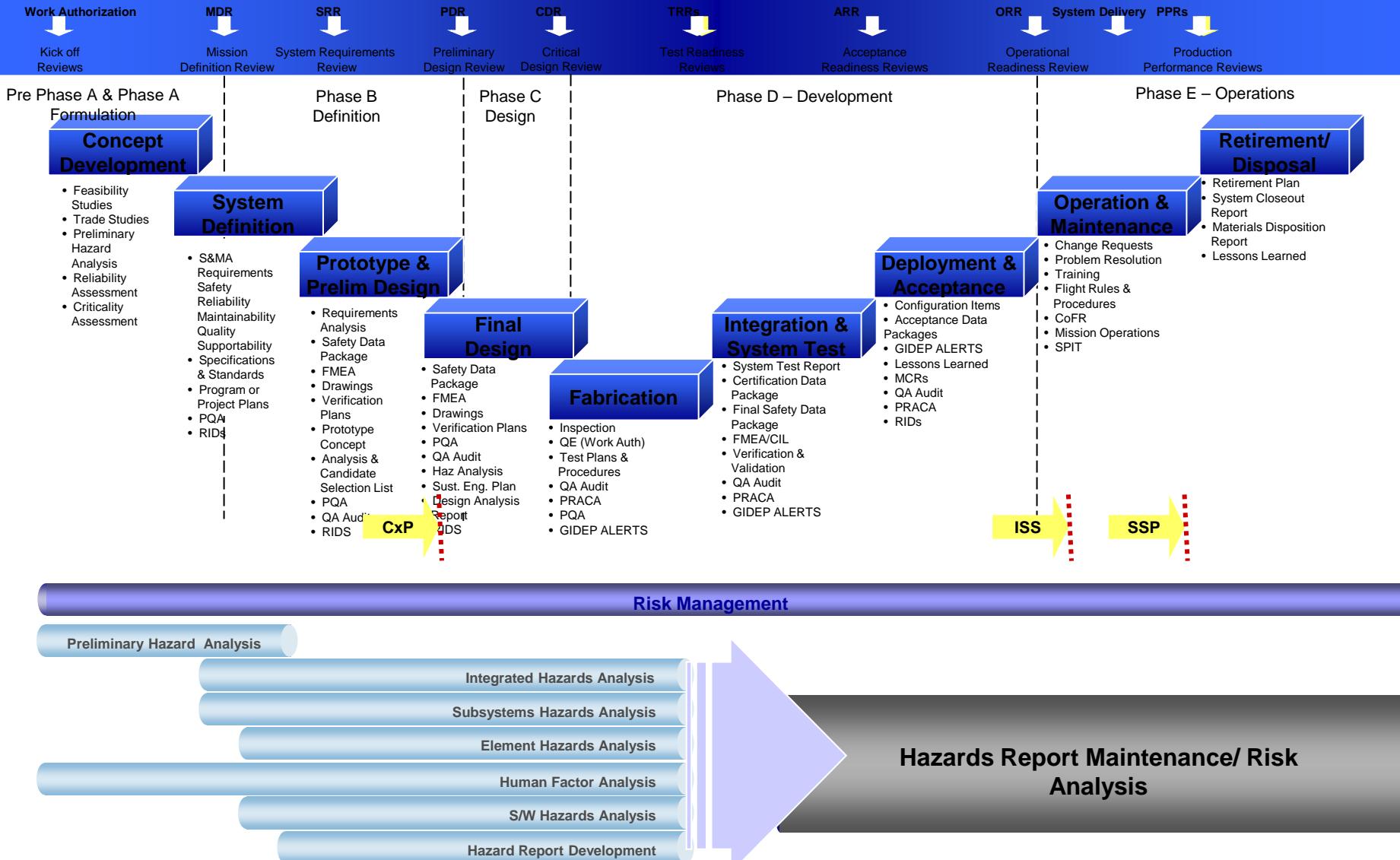
Terry Relyea, NASA
Human Factors Engineering ISS Resolution Team
terry.relyea@nasa.gov

SAIC

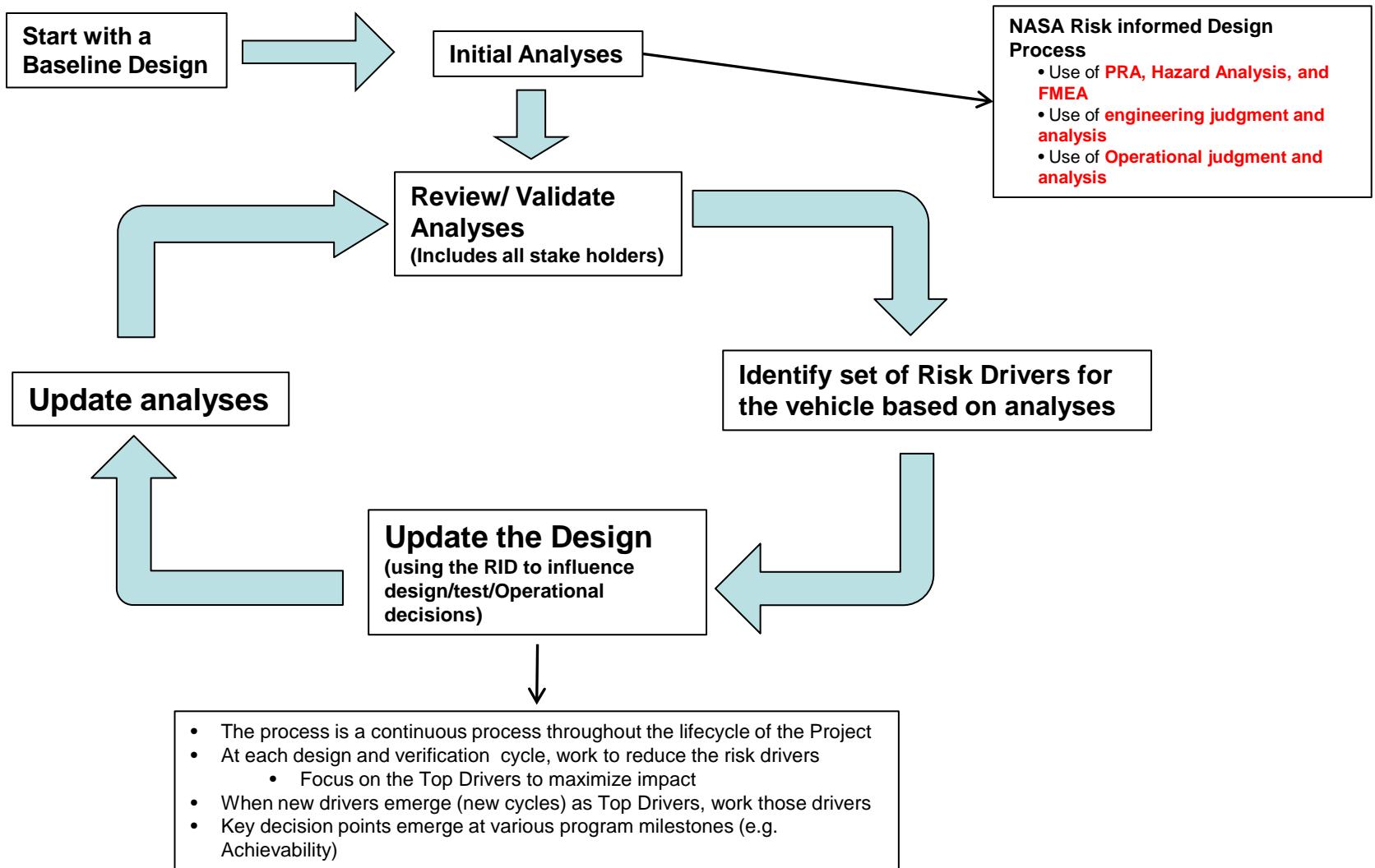


Subsystem Safety Engineering Through the Project Life Cycle

Subsystem Safety Engineering Through the Project Life Cycle



The Risk Informed Design Process



Types of NASA Hazard Analysis



- Preliminary Hazard Analysis
- Subsystem Hazard Analysis
- Element Hazard Analysis
- Operating and Support Hazard Analysis
- Software Hazard Analysis
- Integrated Hazard Analysis
- Functional Hazard Analysis

Preliminary Hazard Analysis (PHA)



- The PHA is the initial effort in hazard analysis during the early design phases that identifies top level hazards and controls, provides a first look at the system risk, and provides the foundation for future analyses. It is based on the best available data. Sources for data include but are not limited to: system description documents, system diagrams, mission descriptions, operational concepts, functional analysis/architecture documents, Functional Flow Block Diagrams (FFBDs), mishap data from similar systems, and lessons learned from other projects. The PHA identifies and evaluates the hazards and hazardous events associated with the proposed design or functions for potential hazard severity, probability, time of exposure, and hazard classification. Design controls, software controls, operational controls and other actions needed to eliminate hazards or reduce the risk to an acceptable level should be considered and documented.

Hazard Analysis Process



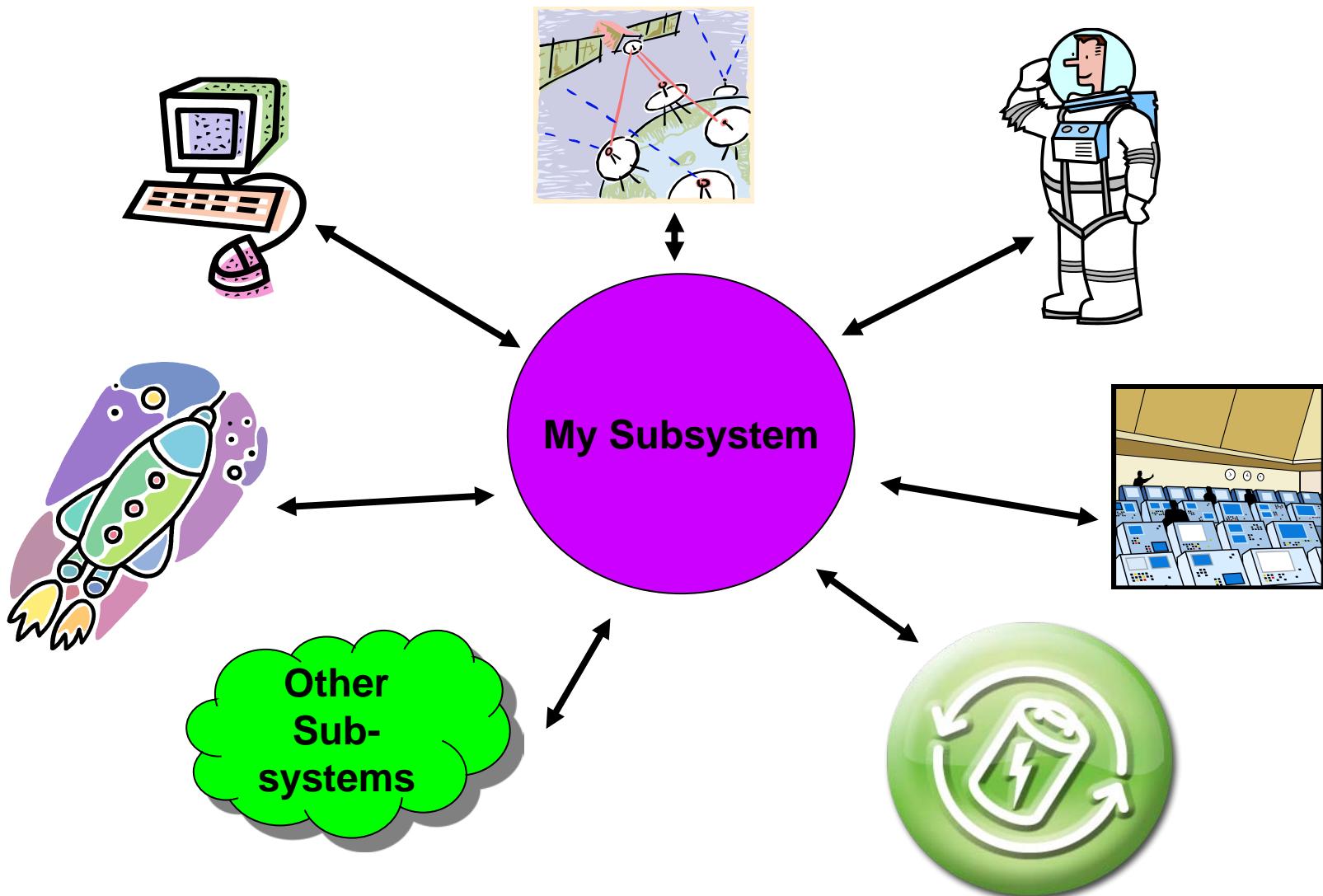
- Identify hazardous conditions, events or states
- Identify the effect of the hazardous state
- Identify severity of the effect
- Identify all potential causes of the hazardous states
- Identify controls for each of the hazard causes
- Identify likelihood of each cause
- Identify verification strategies for the controls
- Track verification to closure

Identify Hazardous Conditions

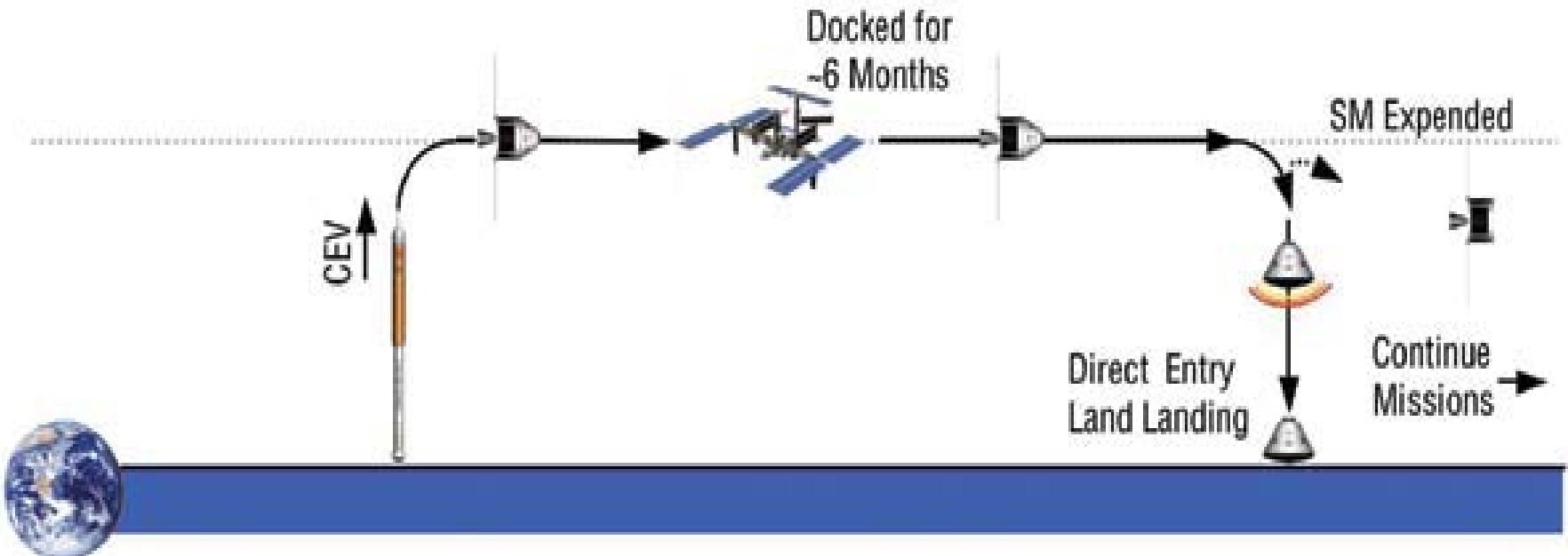


- Basically this is a brainstorming exercise!
- What is inherently dangerous about the operation of your system?
 - Standard hazard lists
 - Historical experience/documentation from legacy systems
 - Your engineering training and experience

Consider all Interfaces



Example



- ISS Crew Transport Mission
 - Launch a crew to the International Space Station
 - Stay docked to the Space Station for 6 months
 - Return the crew to Earth and land in the water

Work a Preliminary Hazard List



- Identify the hazards for this mission.



NASA Generic Hazards List



- Collision or Impacts
- Loss of Control
- Contamination
- Corrosion
- Electrical Discharge/Shock
- Environmental/Weather
- Temperature Extremes
- Gravitational Forces
- Electromagnetic Interference
- Radiation
- Explosion
- Fire/Overheat
- Flight Termination Systems
- Implosion/Loss of Pressure
- High Pressure Sources
- Loss of Structural Integrity
- Mechanical
- Loss of Critical Function
- Loss of Safe Return Capability
- Loss of Habitable Environment
- Pathological/Physiological/
Psychological
- Inadequate HF Engineering
- Lasers
- Utility Outages
- Common Cause Failures

- Hazard analysis results in the identification of risks and the means of controlling or eliminating them. Hazard analysis also quantifies the risk for the Program/Project Manager.





Final Thoughts

- Hazard analysis is structured process to
 - Identify risk
 - Classify risk
 - Manage risk
- Hazard analysis is not an exact science
 - Relies on engineering expertise and engineering judgment
 - Requires rationale to justify hazard classification
- Hazard analysis is an important tool in
 - Design Process
 - Requirements Validation
 - Risk Management